DETAILED ACTION

1. **Claims 1-42** are examined.

Claim Objections

2. Claims 11, 22 and 33 objected to because of the following informalities: Please spell out "***JXTA***".

[Please note that the specification of the invention does not spell out "***JXTA***" either]

Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 6-10, 12-15, 17-21, 23-26, 28-32 and 34-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vigue et al. (US 2003/0163702 A1), referred as "Vigue" hereinafter in view of Winget et al. (US 2005/0120213 A1), referred as "Winget" hereinafter

As per Claim 1, Vigue teaches,

A method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030], the method comprising: the peer node generating a secured communication request to the intermediary peer node [see abstract, lines 3-7, "*… securely sharing resources over a peer-to-peer network generally comprises* ***broadcasting a request by a requesting peer*** *for a resource over the peer-to-peer network where the resource is identified with a resource version identifier*"]; and

the intermediary peer node issuing a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16, "***verifying the retrieved resource*** *by ensuring the retrieved resource contains the version identifier embedded therein. Preferably, the verifying also includes* ***verifying a digital signature****, such as a 1024-bit VeriSign digital certificate, of the retrieved resource to ensure integrity of the retrieved resource*"].

Vigue discloses intermediary peer generating response to said communication request [see FIGS.3-4B; and for example, abstract, lines 8-11, "*receiving a response from a responding peer on the peer-to-peer network indicating that the responding peer has the requested resource,* ***retrieving the requested resource from the responding peer***"], but fails to disclose the intermediary peer node authenticating the peer node in response to said secured communication request.

However, in the same field of endeavor, Winget discloses intermediary peer node authenticating the peer node in response to said secured communication request [see FIG.1; and for example, abstract, "*... shared secret, referred to in this embodiment as the protected access credential may be advantageously used to mutually* ***authenticate a server and a peer*** *upon securing a tunnel for communication via a network...*"].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to combine the teachings of Vigue and Winget because both are in the fields of peer-to-peer network communication systems. Incorporating Winget's teaching of peer node authentication modifies the system of Vigue; so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 12, Vigue teaches,

A method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030], the method comprising: receiving a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses generating response to a secured communication request to the intermediary peer node [see FIGS.3-4B; and for example, abstract, lines 3-11], but fails to disclose authenticating the peer node in response to said secured communication request. However, Winget discloses authenticating the peer node in response to said secured communication request [see FIG.1; and for example, abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of Vigue by incorporating Winget's teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 23, Vigue teaches,

A method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030], the method comprising: receiving a secured communication request from the peer node [see abstract, lines 3-7]; and sending a singed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses generating response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 8-11], but fails to disclose authenticating the peer node. However, Winget discloses authenticating the peer node [see FIG.1; and for example, abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of Vigue by incorporating Winget's teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 34, Vigue teaches,

A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and

0030], the method including: the peer node generating a secured communication request to the intermediary peer node [see abstract, lines 3-7]; and the intermediary peer node issuing a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses intermediary peer node generating response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 8-11], but fails to disclose the intermediary peer node authenticating the peer node. However, Winget discloses peer node authenticating the peer node [see FIG.1; and for example, abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of Vigue by incorporating Winget's teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 35, Vigue teaches,

A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for administrating peer-to- peer networks [see FIGS.1 and 2; and for example, par.0029 and 0030], the method including receiving a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses generating a secured communication request to the intermediary peer node [see FIGS.3-4B; and for example, abstract, lines 3-11], but fails to disclose authenticating the peer node in response to said secured communication request. However, Winget discloses authenticating the peer node in response to said secured communication request [see FIG.1; and for example, abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of Vigue by incorporating Winget's teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 36, Vigue teaches,

A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for administrating peer-to- peer networks [see FIGS.1 and 2; and for example, par.0029 and 0030], the method including: receiving a secured communication request from the peer node [see abstract, lines 3-7]; and sending a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses generating response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 8-11], but fails to disclose authenticating the peer node. However, Winget discloses authenticating the peer node [see FIG.1; and for example, abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of Vigue by incorporating Winget's teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 37, Vigue teaches,

An apparatus for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030] comprising: means for generating a secured communication request to the intermediary peer node [see abstract, lines 3-7], and means for issuing a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses means for generating response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 8-11], but fails to disclose authenticating the peer node. However, Winget discloses authenticating the peer node [see FIG.1; and for example, abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of Vigue by incorporating Winget's teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 38, Vigue teaches,

An apparatus for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030] comprising: means for receiving a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses means for generating a secured communication request to the intermediary peer node [see FIGS.3-4B; and for example, abstract, lines 3-11], but fails to disclose authenticating the peer node in response to said secured communication request. However, Winget discloses authenticating the peer node in response to said secured communication request [see FIG.1; and for example, abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of Vigue by incorporating Winget's teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 39, Vigue teaches,

An apparatus for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030] comprising: means for receiving a secured communication request from the peer node [see abstract, lines 3-7]; and means for sending a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses means for generating response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 8-11], but fails to disclose authenticating the peer node. However, Winget discloses authenticating the peer node [see FIG.1; and for example, abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of Vigue by incorporating Winget's teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 40, Vigue teaches,

A peer-to-peer network system comprising: a peer node [see FIGS.1 and 2]; an intermediary peer node communicatively coupled to said peer node [see FIGS.1 and 2]; wherein said peer node is configured to generate a secured communication request to said intermediary peer node [see abstract, lines 3-7]; and wherein said intermediary peer node is configured to issue a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses wherein said intermediary peer node is configured to generate response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 8-11], but fails to disclose authenticate said peer node. However, Winget discloses authenticate said peer node [see FIG.1; and for example, abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of Vigue by incorporating Winget's teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 41, Vigue teaches,

A peer node comprising: a processor [see FIGS.1 and 2 – *which includes inherent processor*. See also **PROCESSOR 1051** in FIG.10]; and a memory [see **MEMORY 1053** in FIG.10] comprising program instructions, wherein the program instructions are executable by the processor to: generate a

secured communication request to the intermediary peer node capable of authenticating the peer node in response to said secured communication request [see abstract, lines 3-11], and receive a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses generate a secured communication request to the intermediary peer node in response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 3-11], but fails to discloses of authenticating the peer node. However, Winget discloses authenticating the peer node [see FIG.1; and for example, abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of Vigue by incorporating Winget's teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 42, Vigue teaches,

An intermediary peer node comprising: a processor [see FIGS.1 and 2 – *which includes inherent processor.* See also **PROCESSOR 1051** in FIG.10]; and a memory [see **MEMORY 1053** in FIG.10] comprising program instructions, wherein the program instructions are executable by the processor to: send a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses receive a secured communication request from the peer node; and generate response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 3-11], but fails to disclose authenticate the peer node. However, Winget discloses authenticate the peer node [see FIG.1; and for example, abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of Vigue by incorporating Winget's teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claims 2 and 3, Vigue-Winget combination teaches,

wherein said secured communication request comprises a certificate signing request, , wherein said certificate signing request includes a public key cryptography system (PKCS) certificate signing request [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract of **Vigue**], a unique identifier [see **version identifier** in abstract of **Vigue**], and a password [see par.0003, 0007 and 0121 of **Winget**].

Claims 13-14 and 24-25 are rejected for the same reasons applied to the rejection of Claim 3.

As per Claim 4, Vigue-Winget combination teaches,

wherein said secured communication protocol comprises a transport layer data authentication protocol [see **TLS** in FIGS.3 and 4 of **Winget**].

Claims 15 and 26 are rejected for the same reasons applied to the rejection of Claim 4.

As per Claims 6 and 7, Vigue-Winget combination teaches,

securing a pipe connection between the peer node and the intermediary peer node upon authentication [see FIGS.1 and 6 of **Winget**]; and closing said pipe connection upon failed authentication of said node [see **CANCELLING REQUEST 128** in FIG.3 of **Vigue**].

Claims 17-18 and 28-29 are rejected for the same reasons applied to the rejection of Claim 7.

As per Claims 8-10, Vigue-Winget combination teaches,

wherein said peer node comprises a peer node advertisement and a pipe node advertisement; wherein said peer node advertisement comprises a peer node name, a unique peer node identifier, and local transport information [see **TLS** in FIGS.3 and 4 of **Winget**]; and wherein said pipe node advertisement includes an application-dependent port identifier [see **Carrier Protocol** in FIG.3 of **Winget**], said unique identifier, a name, and a type [see FIGS.4 and 5].

Claims 19-21 and 30-32 are rejected for the same reasons applied to the rejection of Claim 8.

Claims 5, 11, 16, 22, 27 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Vigue" in view of "Winget", and further in view of Rutherglen et al. (US 2003/0033517 A1), referred as "Rutherglen", referred as hereinafter

As per Claim 5, Vigue-Winget combination teaches,

authenticating the peer node in response to said secured communication request [see abstracts of Vigue and Wignet], but fails to disclose wherein said intermediate peer node is communicatively coupled to an enterprise database.

However, in the same field of endeavor, Rutherglen discloses wherein said intermediate peer node is communicatively coupled to an enterprise database [see **DATABASE SERVER** in FIGS.1, 2 and 3B-6]. It would have been obvious to modify the system of Vigue-Winget by incorporating the DATABASE SERVER of Rutherglen in order to have a direct access to the database that is protected by a security system [see abstract and par.0001 of **Rutherglen]**.

Claims 16 and 27 are rejected for the same reasons applied to the rejection of Claim 5.

As per Claim 11, Vigue-Winget combination teaches,

operating peer-to-peer network [see abstracts of Vigue and Wignet], but fails to disclose using a JXTA technology-enabled platform. However, Rutherglen discloses using a JXTA technology-enabled platform [see par.0013 and 0108]. It would have been obvious to modify the system of Vigue-Winget by incorporating JXTA teachings of Rutherglen in order to implement a network protocol that would inter-operate with any peer [see par.0109 of **Rutherglen]**.

Claims 22 and 33 are rejected for the same reasons applied to the rejection of Claim 11.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AMARE TABOR whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2139)

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139